National Infrastructure Protection Center CyberNotes

Issue #2001-14 *July 16, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 21 and July 12, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ACLogic[1]	Windows 95/98/ME/ NT 3.5/3.5.1/ 4.0/2000	CaesarFTP 0.98b	A buffer overflow vulnerability exists when the HELP command is sent followed by a very long string of characters, which could let a remote malicious user execute arbitrary code or gain 'SYSTEM' privileges.	No workaround or patch available at time of publishing.	CaesarFTPD FTP Command Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[1] Bugtraq, July 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Allaire[2]	Multiple	ColdFusion Server 2.0- 4.5.1 SP2	Two vulnerabilities exist: one could let a remote malicious user gain unauthorized read and delete access to files; and the second could let a remote malicious user corrupt the data in template files by creating a new file with the same name as an existing template.	Patch and FAQ available at: http://www.allaire.com/handlers/index.cfm?id=21579	ColdFusion Template Overwrite	Medium	Bug discussed in newsgroups and websites.
Allaire[3]	Windows 95/98/ NT 4.0/2000, Unix	JRun 2.3.x, 3.0	A vulnerability exists because JRun does not filter script embedding from links that are displayed on a server's website, which could let a malicious user cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyperlink.	Patch available at: http://download1.allaire.com/publicdl/en/jrun/	JRun Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Apache Group[4]	Unix	Tomcat 3.2.1	A vulnerabilty exists because Apache Tomcat does not filter script embedding from links that are displayed on a server's website, which could let a malicious user cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyperlink.	No workaround or patch available at time of publishing.	Tomcat Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Apache Group[5]	Unix	Apache 1.3.11, 1.3.14, 1.3.17-1.3.20	A vulnerability exists in the 'index.html' module, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Apache Autoindexing Module Directory Index Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Apple[6]	MacOS X 10.0-10.0.4	MacOS X 10.0-10.0.4	A vulnerability exists in the 'nidump' program, which could let a malicious user gain access to the password file.	No workaround or patch available at time of publishing.	MacOS X 'nidump' Password File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
ArGoSoft[7]	Windows 95/98/ME/ NT 4.0/2000	ArGoSoft FTP Server 1.0, 1.2.2.2	A directory traversal vulnerability exists, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	ArGoSoft FTP Server .lnk Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Basilix[8]	Unix	Webmail 1.02beta, 1.03beta	A vulnerability exists due to improperly filtered user-supplied input, which could let a remote malicious user gain sensitive information.	The vendor has posted details on how to fix it at: http://basilix.org/index.php3?page=home&lang=en	Webmail File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[2] Macromedia Product Security Bulletin, MPSB01-07, July 11, 2001.
[3] Macromedia Product Security Bulletin, MPSB01-06, June 28, 2001.
[4] Bugtraq, July 2, 2001.
[5] SecurityFocus, July 10, 2001.
[6] Securiteam, July 8, 2001.
[7] Securiteam, July 4, 2001.
[8] Bugtraq, July 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BisonFTP[9]	Windows 95/98/NT 4.0/2000	Bison FTP Server V4R1	A directory traversal vulnerability exists which could let a malicious user gain sensitive information.	Upgrade available at: http://www.bisonftp.com/Files/BisonFTP42.exe	BisonFTP BDL File Upload Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Caucho Technology[10]	Unix	Resin 1.2.2	A vulnerabilty exists because script embedding is not filtered from links that are displayed on a server's website, which could let a malicious user cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyper-link.	Upgrade to a later version available at: http://www.caucho.com/download/	Resin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Cayman[11]	Multiple	3220-H DSL Router 1.0	A vulnerability exists due to an insecure user account, which could let a remote malicious user gain access to the device's configuration.	No workaround or patch available at time of publishing.	Cayman-DSL Router Insecure Default	Medium	Bug discussed in newsgroups and websites.
Cayman[12]	Multiple	Cayman 3220-H DSL Router 1.0	A Denial of Service vulnerability exists when a malicious user sends a number of TCP connect() requests or SYN packets to the device.	No workaround or patch available at time of publishing.	Cayman-DSL Router Portscan Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

Check Point Software Technologies[13]	Multiple	VPN-1 4.1- 4.1SP3;
		Software Providor-1 4.1 4.1SP3;
		Firewall-1 4.1- 4.1SP3;
		Nokia ISPO 3.3- 3.3SP2
			A vulnerability exists due to improper string formatting in the client-supplied data to a printf* function, which could let a remote malicious user cause a Denial of Service or execute arbitrary bode. Only a client that has authenticated as an administrator can exploit this vulnerability.	Update available at: http://www.checkpoint.com/techsupport/downloads/downloads.html	Firewall-1/ VPN-1 Management Station Format String	Low/**High**	Bug discussed in newsgroups and websites.

[9] Securiteam, July 5, 2001.
[10] Bugtraq, July 2, 2001.
[11] Bugtraq, July 11, 2001.
[12] Bugtraq, July 9, 2001.
[13] eSecurityOnline Free Vulnerability Alert 3784, July 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Check Point Software Technologies[14]	Multiple	Firewall-1 4.1 SP2 Build 41716, 4.1 Build 41439, 4.1	A directory traversal vulnerability exists which could let a remote malicious user pass packets across the firewall via port 259 by using false RDP (Reliable Data Protocol) headers on UDP packets. This makes it possible for remote users to gain access to restricted information systems. Not only can such access be gained with a Trojan horse that uses this vulnerability to connect from the inside back to the machine of the attacker, but also arbitrary connections from the outside to machines behind the firewall (even if they are supposedly totally blocked from inside and outside by the firewall) can be established.	Hotfix available at: http://www.checkpoint.com/techsupport/downloads.html	Firewall-1 RDP Header Firewall Bypassing	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

Cisco Systems[15]	Multiple	All devices running Cisco IOS software supporting SSH;
		Catalyst 6000 switches running CatOS;
		Cisco PIX Firewall
			Three vulnerabilities exist: a CRC-32 integrity check vulnerability; a traffic analysis vulnerability; and a key recovery in SSH protocol 1.5 vulnerability, which could let a malicious user insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.	Upgrade available at:
				http://www.cisco.com
					Cisco Multiple SSH Vulnerabilities	Medium/ **High**	Bug discussed in newsgroups and websites.
							Vulnerability has appeared in the press and other public media.

Cisco Systems[16]	Multiple	SN 5420 Storage Router 1.1(3)	Two vulnerabilities exist: a vulnerability in the default configuration of the router could let a remote malicious user gain unauthenticated access; and a Denial of Service vulnerability occurs when multiple connections are rapidly established to TCP port 8023.	Software upgrades that rectify this issue are available and can be obtained by contacting Cisco at: http://www.cisco.com	Cisco SN 5420 Storage Router Developer Access and Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites.
Cisco Systems[17] ***Exploit script released***[18]	**Multiple**	**IOS 11.3 & later**	**A vulnerability exists with the HTTP server component of Cisco IOS system software, which could let a remote malicious user gain full administrative privileges if local authentication databases are used.**	**For upgrade information see advisory located at:** **http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html**	**Cisco IOS HTTP Configuration Arbitrary Administrative Access**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***

[14] Inside Security GmbH Vulnerability Notification, Revision 1.2, July 9, 2001.
[15] Cisco Security Advisory, June 27, 2001.
[16] Cisco Security Advisory, CI-01.09, July 11, 2001.
[17] Cisco Security Advisory, June 27, 2001.
[18] Securiteam, July 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[19]	Multiple	IOS 12.1 train, releases: T, E, EZ, YA, YD and YC; IOS 12.2 train, all releases	A vulnerability exists when a malformed Point to Point Tunneling Protocol (PPTP) is sent to port 1723, which could let a remote malicious cause a Denial of Service.	Upgrade available at: http://www.cisco.com/warp/public/707/PPTP-vulnerability-pub.html#Software	Cisco IOS Malformed PPTP Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
Citrix[20]	Multiple	Nfuse 1.51	A vulnerability exists when a request is submitted to the launcher application without specifying the required information, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Nfuse Webroot Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Cobalt[21]	Unix	RaQ 3.0	A vulnerability exists in PopRelayD because it doesn't authenticate output to the /var/log/maillog file, which could let a remote malicious user add themselves to the 'allowed to relay' list using a specially crafted SMTP command.	No workaround or patch available at time of publishing.	RaQ PopRelayD Arbitrary SMTP Relay	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Connect, Inc.[22]	Unix	PowerNet IX Debian 6.0	A Denial of Service vulnerability exists when ports on Powernet IX are scanned.	No workaround or patch available at time of publishing.	Powernet Portscan Denial of Service	Low	Bug discussed in newsgroups and websites. No exploit is required.
EnGarde[23]	Unix	Secure Linux 1.0.1	A vulnerability exists in the configuration file for the 'sudo' package, which could let a malicious user gain elevated privileges.	No workaround or patch available at time of publishing.	EnGarde 'sudo' Privileged Command Execution	Medium	Bug discussed in newsgroups and websites.
FreeBSD[24]	Unix	FreeBSD 4.0-4.3	A vulnerability exists in the exec() implementation because the system calls fails to prevent signal handlers from being inherited by processes attempting to exec setuid images, which could let a malicious user execute arbitrary code with elevated privileges.	No workaround or patch available at time of publishing.	FreeBSD exec() Inherited Signal Handler	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Grant Averett[25]	Windows	Ceberus FTP Server 1.0-1.3, 1.5	A Denial of Service vulnerability exists when a large number of 'PASV' requests are sent.	No workaround or patch available at time of publishing.	Cerberus FTP Server 'PASV' Denial of Service	Low	Bug discussed in newsgroups and websites.

[19] Cisco Security Advisory, CI-01.10, July 12, 2001.
[20] Securiteam, July 7, 2001.
[21] Securiteam, July 9, 2001.
[22] SecurityFocus. June 29, 2001.
[23] EnGarde Secure Linux Security Advisory, ESA-20010711-02, July 11, 2001.
[24] Georgi Guninski Security Advisory #48, July 10, 2001.
[25] Bugtraq, July 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[26]	Windows 98/NT 2000	IBM DB2 Universal Database for Windows	A remote Denial of Service vulnerability exists when a malicious user Telnets to port 6789 or 6790 and sends one byte of data.	Vendor has been notified and a patch should be available in late July.	DB2 Denial of Service	Low	Bug discussed in newsgroups and websites. No exploit is required.
IBM[27]	Windows NT 4.0, Unix	WebSphere Application Server 3.0.2, 3.5	A vulnerability exists because script embedding is not filtered from user-submitted links that are displayed on the server's websites. A malicious webmaster can exploit this vulnerability to cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyperlink.	Patch available at: http://www-4.ibm.com/software/webservers/appserv/efix.html	WebSphere Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
John Bovey[28]	Unix	xvt 2.1	A buffer overflow vulnerability exists when parsing large arguments to the '-T' and '-name' commandline options, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Xvt Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Jon Zeeff[29]	Multiple	lmail 2.7	A race condition vulnerability exists due to insecure use of temporary files, which could let a malicious user overwrite any file on a system with arbitrary data.	No workaround or patch available at time of publishing.	Lmail Temporary File Race Condition	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Lee Herron[30]	Unix	All Commerce 1.2.3	A vulnerability exists because files are created in the /tmp directory insecurely, which could let a malicious user elevate his/her privileges.	Upgrade available at: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/	AllCommerce Symlink	Medium	Bug discussed in newsgroups and websites.
Lotus[31]	Windows NT 4.0/2000, Unix, OS/390 V2R9, OS/2 4.5Warp	Lotus Domino 5.0.6	A vulnerability exists if specially crafted text is appended to a URL, which could let a malicious user execute arbitrary code.	Lotus has knowledge of this issue and will be addressing it in Domino R5.0.9. Lotus's SPR associated with this vulnerability is JCHN4V2HUY.	Lotus Domino Server Cross Site Scripting	High	Bug discussed in newsgroups and websites.
Max Feoktistov[32]	Windows 95/98	Small HTTP server 1.212, 2.01, 2.03, 3.0 beta	A Denial of Service vulnerability exists when URLs containing long strings of arbitrary text are submitted repeatedly.	No workaround or patch available at time of publishing.	SmallHTTP Server Long URL Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Bugtraq, July 11, 2001.
[27] Bugtraq, July, 2, 2001.
[28] Securiteam, July 7, 2001.
[29] Bugtraq, July 5, 2001.
[30] EnGarde Secure Linux Security Advisory, ESA-20010711-01, July 11, 2001.
[31] Bugtraq, July 2, 2001.
[32] Bugtraq, June 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
McAfee[33]	Windows NT 4.0/2000	ASaP Virusscan 1.0	A directory traversal vulnerability exists which could let a malicious user gain sensitive information	No workaround or patch available at time of publishing.	ASaP Virusscan Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[34]	Windows 2000	Windows 2000, 2000 SP1 & SP2	A vulnerability exists in the authentication process of the SMTP service, which could let a remote malicious host successfully authenticate and use the SMTP services as an authenticated user.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-037.asp	Microsoft Windows 2000 SMTP Improper Authentication CVE Name: CAN-2001-0504	Medium	Bug discussed in newsgroups and websites.
Microsoft[35]	Windows NT 4.0/2000	Office XP	A vulnerability exists due to a new ActiveX control called 'Microsoft Outlook View Control', which could let a malicious user access and manipulate user e-mail and execute arbitrary commands.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-038.asp	Microsoft Office XP Unauthorized E-mail Access and Arbitrary Code Execution CVE Names: CAN-2001-0538; CAN-2001-0538	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[36]	Windows NT 4.0/2000	IIS 4.0, 5.0	A Denial of Service vulnerability exists when opening and reading device files (com1, com2, etc.) using the Scripting.FileSystem Object.	Microsoft's response: "To address this specific issue, the IIS4 and 5 checklists include a recommendation to remove the FSO component - I believe the IIS5 security configuration tool also removes this mapping automatically." Please see the Credit section for IIS 4 and 5 security checklists located at: **IIS 4:** http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/iischk.asp **IIS 5:** http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp	Microsoft IIS Device File Local Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[33] Securiteam, July 12, 2001.
[34] Microsoft Security Bulletin, MS01-037, July 5, 2001.
[35] Microsoft Security Bulletin, MS01-038, July 12, 2001.
[36] NERF gr0up security advisory #4, July 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[37]	Multiple	Merit 3.6b RADIUS Lucent 2.1-2 RADIUS	Several buffer overflow vulnerabilities exist in the authentication routines, which could let a remote malicious user execute arbitrary code and potentially gain local root access.	**Merit:** ftp://ftp.merit.edu/radius/releases/radius.3.6B1.basic.tar.gz **Lucent:** ftp://ftp.vergenet.net/pub/lucent_radius/	Merit RADIUS and Lucent RADIUS Multiple Buffer Overflows CVE Name: CAN-2001-0534	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[38]	Windows NT 4.0/2000, Unix	xloadimage 4.1	A buffer overflow vulnerability exists in the way the 'Faces Project' image type is handled, which could let a malicious user execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/6.2/en/os/	xloadimage Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[39]	Windows NT 4.0/2000, Unix	Sun Solaris 2.5.1, 7.0, 8.0; OpenBSD 2.8, 2.9; NetBSD 1.5, 1.5.1; Microsoft Windows NT 4.0, 4.0 SP1-SP7, Windows 2000, 2000 SP1&SP2; Linux Kernel 2.4-2.4.5; HP-UX 11.0, 11.0.4, 11.11, 11.4; FreeBSD 4.3	A potential Denial of Service vulnerability exists in several TCP stack implementations because only a small minimum value is enforced for the MSS (maximum segment size) option that is used by a TCP client.	No workaround or patch available at time of publishing.	Multiple Vendor Small TCP MSS Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[40, 41]	Unix	OpenSSL 0.9.1c, 0.9.2b, 0.9.3-0.9.6a; SSLeay 0.8.1-0.9.1	A vulnerability exists in the pseudo-random number generator (PRNG), which could let a malicious user predict future PRNG output and reconstruct the generator's internal state.	**Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Engarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/	OpenSSL PRNG Internal State Disclosure	Medium	Bug discussed in newsgroups and websites.
Network Appliance[42]	Multiple	NetCache C1100, C3100, C6100, C700 Series	A vulnerability exists in the default configuration, which could let a remote malicious user tunnel through the appliance to arbitrary ports on any remote system.	No workaround or patch available at time of publishing.	NetCache Tunneling Configuration	Medium	Bug discussed in newsgroups and websites.

[37] Internet Security Systems Security Advisory, ISS-087, July 5, 2001.

[38] Bugtraq, July 10, 2001.

[39] Bugtraq, July 8, 2001.

[40] Trustix Secure Linux Security Advisory, 2001-0012, July 11, 2001.

[41] EnGarde Secure Linux Security Advisory, ESA-20010709-01, July 9, 2001.

[42] Bugtraq, July 5, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[43]	Multiple	Opera Web Browser 5.0 Linux	A heap overflow vulnerability exists which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Opera Heap Overflow	**High**	Bug discussed in newsgroups and websites.
PHP Development Team[44]	Multiple	PHP 4.0.5	A vulnerability exists in the toolkit, which could let a malicious user elevate his/her privileges and execute arbitrary code.	Upgrade available at: http://www.php.net/do_download.php?download_file=php-4.0.6.tar.gz&source_site=www.php.net	PHP SafeMode Arbitrary File Execution	**High**	Bug discussed in newsgroups and websites.
PhpPg Admin[45]	Unix	PhpPg Admin 2.2, 2.2.1, 2.2.1pl1; PhpMy Admin 2.1	An input validation vulnerability exists in the include() function, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.greatbridge.org/pub/phppgadmin/stable/phpPgAdmin_2-3.tar.gz	PhpPgAdmin and PhpMyAdmin Included File Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
PhpSecure Pages[46]	Multiple	PhpSecure Pages 0.11beta-0.20beta	An input validation vulnerability exists in the 'cfgProgPath' variable, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.bnr.nl/bigdeal/download/phpSecurePages.zip	PhpSecure Pages Included File Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
Squirrel Mail[47]	Unix	SquirrelMail 1.0.4, 1.0.5	An input validation vulnerability exists in the include() function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/squirrelmail/squirrelmail-1.0.6.tar.gz	SquirrelMail Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[48]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in 'whodo', which could let a malicious user gain root privileges.	Sun is aware of the problem and fixes are reportedly forthcoming.	Solaris 'whodo' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
TransSoft[49]	Windows 95/98/ME/ NT 4.0/2000	Broker FTP Server 3.0 Build 1, 3.0x, 4.0, 4.7.5.0, 5.0, 5.1, 5.7, 5.7.5, 5.9.5.0	A directory traversal vulnerability exists, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Broker .lnk Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro[50]	Windows NT 4.0/2000	InterScan Web Manager 1.2	A buffer overflow vulnerability exists in HttpSave.dll, which could let a remote malicious user execute arbitrary code.	Trend Micro is aware of this vulnerability and it will reportedly be fixed in the next release of Interscan WebManager.	InterScan WebManager HttpSave.dll Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[43] SecurityFocus, July 9, 2001.
[44] Bugtraq, June 30, 2001.
[45] Secure Reality Pty Ltd. Security Advisory, SRADV00008, July 3, 2001.
[46] Secure Reality Pty Ltd. Security Advisory, SRADV00009, July 3, 2001.
[47] Secure Reality Pty Ltd. Security Advisory, SRADV00010, July 3, 2001.
[48] Bugtraq, July 5, 2001.
[49] Securiteam, July 4, 2001.
[50] SNS Advisory No.36, July 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Trend Micro[51]	Windows NT 4.0/2000	InterScan VirusWall 3.51	A buffer overflow vulnerability exists in smtpscan.dll, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.antivirus.com/download/register.asp?product_id=1&product_from=isvw&page=product	InterScan VirusWall HttpSave.dll Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Trend Micro[52]	Windows NT 4.0/2000	InterScan VirusWall 3.51	A buffer overflow vulnerability exists in HttpSaveC*P.dll, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.antivirus.com/download/register.asp?product_id=1&product_from=isvw&page=product	InterScan VirusWall 3.51 HttpSaveC*P. dll Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Trend Micro[53]	Windows NT 4.0/2000, Unix	Interscan Applet Trap 2.0	Multiple bypass vulnerabilities exist: a vulnerability exists when a certain number of '0' are affixed to the IP address; when encoding all or a few characters of an unauthorized URL; and by affixing an additional '/' to an unauthorized URL, which could let a malicious user bypass restrictions.	No workaround or patch available at time of publishing.	Multiple InterScan Applet Trap Bypass Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Tripwire[54]	Unix	Tripwire 1.3.1, 2.2.1, 2.3.0	A vulnerability exists because temporary files are opened and created insecurely, which could let a malicious user gain elevated privileges.	Upgrade available at: http://prdownloads.sourceforge.net/tripwire/tripwire-2.3.1-2.tar.gz	Tripwire Insecure Temporary File Symbolic Link	Medium	Bug discussed in newsgroups and websites.
VWeb Server[55]	Windows 95/98/NT 4.0/2000	vWebServer 1.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when URLs containing long strings of arbitrary text are submitted repeatedly; a Denial of Service vulnerability exists when submitting a request to the webserver including the 'AUX' MS-DOS device name; and a source code vulnerability exists if a Unicode-format space character is appended to a URL which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	vWebServer Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[51] SNS Advisory No.34, June 28, 2001.
[52] SNS Advisory No.35, June 28, 2001.
[53] eDvice Security Services Advisory, July 9, 2001.
[54] Securiteam, July 10, 2001.
[55] Bugtraq, June 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xinetd[56, 57, 58, 59, 60,]	Unix	Xinetd 2.1.8.8, 2.1.8.8pre3, 2.1.8.9pre1-2.1.8.9pre9	A buffer overflow vulnerability exists due to improper handling of string data in some internal functions, which could let a malicious user gain root privileges.	Update available at: **Immunix:** http://download.immunix.org/ImmunixOS/7.0/updates/ **EnGarde Secure Linux:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/6.0/ **RedHat:** ftp://updates.redhat.com **Mandrake:** http://www.linux-mandrake.com/en/ftp.php3	Xinetd Zero String Length Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 2 and July 12, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 18 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

[56] Immunix OS Security Advisory, IMNX-2001-70-029-01, June 29, 2001.
[57] EnGarde Secure Linux Security Advisory, ESA-20010621-01, June 21, 2001.
[58] Conectiva Linux Security Announcement , CLA-2001:406, June 30, 2001.
[59] Red Hat Security Advisory, RHSA-2001:092-02, July 6, 2001.
[60] Mandrake Linux Security Update Advisory, MDKSA-2001:055-1, July 5, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
July 12, 2001	**Libsldap-exp.c**	**Exploit script for the Solaris Libsldap Buffer Overflow vulnerability.**
July 12, 2001	**Mcaffee.mycio.traversal.txt**	**Exploit URL for the McAffee's MyCIO Directory Traversal vulnerability.**
July 12, 2001	Tstot.c	Script which exploits the xloadimage Buffer Overflow vulnerability.
July 12, 2001	**Vvfreebsd.c**	**Script which exploits the FreeBSD exec() Inherited Signal Handler vulnerability.**
July 12, 2001	Vvopenbsd.c	Script which exploits the OpenBSD Race Condition vulnerability.
July 12, 2001	**Whodo-ex.c**	**Exploit script for the Solaris 'whodo' Buffer Overflow vulnerability.**
July 10, 2001	Lcrzosrc-3.14.tgz	A toolbox that contains over 200 functionalities which can be used to sniff, spoof, create clients/servers, create decode and display packets.
July 10, 2001	Ngrep-1.40.tar.gz	A network sniffing tool that will allow you to specify extended regular expressions to match against data payloads of packets.
July 10, 2001	Nmap-2.54BETA26.tgz	A utility for port scanning large networks.
July 10, 2001	Ntop-beta-2105.tgz	Unix / Windows network sniffing tool that shows the network usage.
July 10, 2001	Xloadimageexp.c	Script which exploits the xloadimage Buffer Overflow vulnerability.
July 9, 2001	Ettercap-0.5.2.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
July 8, 2001	**Maxseg.c**	**Script which exploits the Multiple Vendor Small TCP MSS Denial of Service vulnerability.**
July 6, 2001	Cisco.c	Script which exploits the Cisco IOS HTTP Configuration Arbitrary Administrative Access vulnerability.
July 5, 2001	**Lmail-xpl.c**	**Script which exploits the Lmail Temporary File Race Condition vulnerability.**
July 4, 2001	Aspexploit.txt	Technique for exploiting the Microsoft IIS Device File Local Denial of Service vulnerability.
July 2, 2001	Log.c	Script which exploits the Xinetd Zero String Length Buffer Overflow vulnerability.
July 2, 2001	**Xvt-exp.c**	**Script which exploits the Xvt Buffer Overflow vulnerability.**

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- A bogus Microsoft Bulletin spreads the Internet worm, W32.Leave.B.Worm. For more information, please see the Trojan Section.

- Two network-aware viruses, PE_Funlove.4099 and PE_Magistr.A, have resurfaced and are spreading at a rapid rate.
- **The NIPC and FedCIRC have recently received information on attempts to locate, obtain control of and plant new malicious code known as "W32-Leaves.worm" on computers previously infected with the SubSeven Trojan. For more information, see ADVISORY 01-014, located at: http://www.nipc.gov/warnings/advisories/2001/01-014.htm.**
- A worm called DoS.Storm.Worm seeks out Microsoft Internet Information Services (IIS) systems that have not applied the proper security patches. Any systems that the worm finds are then infected with the worm. The payload of this worm performs a Denial of Service attack on www.microsoft.com (See Virus Section).
- Recent reports on IIS vulnerabilities and the large amount of NT servers being penetrated using different exploits have raised the need to tighten the security of IIS version 5.0 servers. Please see the IIS version 5.0 checklist at: http://www.microsoft.com/technet/security/iis5chk.asp.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

HTML.Reality.B: When the virus is first executed, it modifies the registry so that the security check is disabled and it infects .htt, .asp, .htm, and .html files in the current folder and in several subfolders under the \Windows and \Program Files folders. Whenever the virus is executed, there is a 50% chance that the first payload, which drops a parasitic .com infector, will activate. However, due to a number of bugs, the payload is never executed. On the 5th, 15th, and 30th of any month, the second payload activates. This payload changes the following registry settings:

- ProductName
- RegisteredOwner
- RegisteredOrganization
- Start Page

These settings are changed to ones that contain profane language.

VBS_HAPTIME.B (Aliases: HAPTIME, HAPTIME.B) (Visual Basic Script Worm): This Visual Basic Script (VBS) worm propagates via Microsoft Outlook Express 5.0 by configuring the default stationery to an external file that is dropped by this worm when it is executed. To infect, it appends itself as an embedded script to an infected file. If the current day and the current month are equal to 13, it deletes all .DLL and .EXE files on the local and network drives.

VBS/Niloj-A (Alias: VBS.Jolin@mm) (Visual Basic Script Worm): This is a Visual Basic Script worm that attempts to copy itself to a file called !!jolin_caught_naked!!!!.jpg.vbs in both the Windows and Windows System directories. If mIRC (Internet Relay Chat) or Microsoft Outlook are installed, the worm then tries to use these applications to spread. It may also attempt to overwrite files in the Windows System and My Documents directories with itself.

W32.Efortune.28672@mm (Alias: I-Worm.Roach.b) (Win32 Worm): This is an encrypted mass mailer with backdoor capabilities. It uses IRC to spread. It is an older variant of the mass mailer W32.Efortune.31384@mm with much of the latter's functionality, except for the following differences. This variant:

- Is encrypted with a simple encryption method
- Does not have the virus infection routines that the newer variant does
- Inserts itself into the host's \System folder as Dccom32.exe along with the file Eggcase.att, which is a zip file that contains the files File_id.diz and Cookie.exe

- Checks for the last four characters of its own file name as being either "okie" or "om32" before deciding what to do
- Creates the value dcomdriver = <path>\dccom32.exe in the registry \Run key
- Sends e-mail with the attachments Setup.exe and Fortune.zip
- Has bugs that may cause it to crash on some systems when there are no network connections

W32.HLLC.Abessive: (Win32 Virus): This virus is a companion infector. It infects files by renaming the host file and then copying itself to the system using the host's original file name. When the virus is first executed, it immediately runs the renamed host file, if it exists. If the virus file name is not included in the following list, or if the renamed host file no longer exists, then no secondary file will be executed, but the virus will still replicate. It then searches all folders on all hard disks from C to Z, and looks for any of the following file names:

- iexplore.exe
- Mspaint.exe
- Winhelp.exe
- Winhlp32.exe
- Winword.exe
- Excel.exe

If the virus finds any of these files, it adds an underscore (_) to the file name and it then copies itself to the hard disk using the host's original file name.

W32.Lad.1916 (Aliases: W32.ADT, Win32.ADT(Win32 Virus): This is a virus that runs on all Windows 32-bit platforms (95/98/ME/NT/2000). It is a direct infector, and it infects Microsoft Portable Executable (PE) files. When executed, the virus does not go memory resident. Instead, the virus attempts to infect files in the \Windows and the \Windows\System folders, as well as files in the same folder as the virus. Its payload is executed on the 19th of every month, and it displays a short message.

W32/Marijuana (Aliases: I-Worm.Mari, W32/Mari) (Win32 Worm): This is a worm that attempts to e-mail itself to entries in the Microsoft Outlook address book with the subject "check this out!!!." The worm copies itself to system32.exe in the Windows directory, and sets the registry key HKLM\Software\ Microsoft\Windows\CurrentVersion\Run\System32 to point to the copy, so that it runs on every reboot. The worm sets the Internet Explorer home page to http://my.marijuana.com and changes the Windows registered owner to "Im A Pot Head!," and the organization to "Stoner's Pot Palace." It puts an icon of a marijuana leaf in the system tray. When the user clicks on the icon, it displays a message box with a long statement about legalizing marijuana. Each day at 16:20, it displays a message box with the title "The Marijuana Virus!!" and the message "It's 4:20, Time to toke up :)"

W32.Mineup.Worm (Win32 Worm): This is a worm that is spread by disguising itself as an update to the popular Windows game Minesweeper. The worm consists of two components, one executable component and one VBS component. The VBS component sends the executable file to everyone in your Microsoft Outlook Address Book. The worm also contains a small payload routine that executes on the 15th of every month. It is written in a High-Level Language (HLL).

W97M.Claud.Gen (Aliases: W97M/Claud, W97M/Claud.gen) (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. It does not have a destructive payload. When a document that is infected with W97M.Claud.Gen , it may change the following Word options:

- When you open a document that contains a macro, the warning message no longer appears by default.
- The menu option that controls macro settings is disabled.

W97M.Iseng.Gen (Alias: W97M/Iseng.gen) (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot.
The virus will rewrite any macros contained in the documents. W97M.Iseng.Gen changes the following settings in Microsoft Word:

- When a macro is run, Word will not display any prompts or alert messages.

- Auto-macros are enabled.
- The menu command that allows you to change macro settings is disabled.
- The menu command for the Visual Basic Editor is disabled.
- When you press the key combination that starts the Visual Basic Editor or invoke the macro settings command, the macro virus displays one of the following messages:
  Visual Basic Editor Error: Please reinstall your Microsoft Office Program
  Macro Editor Error: Please reinstall your Microsoft Office Program
- When the Tools > Options or Help > About menu commands are chosen, W97M.Iseng.Gen may display some text in the Indonesian language.

W97M_MSKONG.A (Aliases: MSKONG, MSKONG.A): (Word 97 Macro Virus): This non-destructive Word macro virus infects documents that are opened. It then resides in the ThisDocument and MSKONG modules. It consists of the macros AutoOpen, AutoClose, FileSaveAs, ToolsMacro, ViewVBCode, FileOpen, ToolsOption, and FileTemplates.

W97M.Odious.F (Alias: W97M/Odious) (97 Word Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. When a document that is infected with W97M.Odious.F is opened or closed, the macro virus changes the following Microsoft Word settings:

- The Ctrl+Break key combination is disabled. This prevents you from interrupting a macro.
- When you run a macro, Word will not display any prompts or alert messages.

If the Visual Basic Editor is displayed during the macro virus activation, or if the installed Word version is Word 2002 (part of Microsoft Office XP), then the macro virus does not replicate; instead it rewrites the Autoexec.bat file with the following string: "Deltree C:\*.* /y." This deletes everything from drive C the next time that you restart the computer. The macro virus then closes Microsoft Word.

W97M.Smac.Gen (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the global template, Normal.dot. When a document that is infected with W97M.Smac.Gen is opened or closed, the macro virus uses the temporary file C:\Bdoc2.txt to replicate itself into active documents and the Normal.dot template.

WM97/Marker-GR (Word 97 Macro Virus): This is a corrupted variant of the WM97/Marker-C Word macro virus. Whenever a document is closed, the virus attempts to FTP information about the infected user from Word to a site ostensibly belonging to the hacking group Codebreakers. It also appends this information to the bottom of the macro as comments.

WM97/Myna-AT (Word 97 Macro Virus): This is a Word macro virus that contains no intentionally malicious code. The replicating code contains the text 'MYNAMEISVIRUS,' which is used as a flag to check for its presence.

WM97/Proverb-S (Word 97 Macro Virus): This is a member of the WM97/Proverb Word macro virus family. This virus may display a message box containing text with Russian characters, or use the Microsoft Office Assistant to display a similar message.

WM97/Twopey-A (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. The virus modifies the File Summary Information of infected documents, changing the Author field to "OPEY A." and the Document Title field to "OpeY 2k1 version - Philippines." The virus also disables access to the Visual Basic Editor.

WM97/Wrench-P (Word 97 Macro Virus): This is a Word macro virus. If the user tries to change the document font or print the document, the virus will display the Office Assistant. If the user tries to view the VBA code, it will display a VBA error. The non-viral file "ascii.vxd," containing the virus code in text form, is dropped in the root directory.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AOL.PWSteal.86016	**N/A**	**Current Issue**
Artic	**0.6 beta**	**Current Issue**
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	**N/A**	**Current Issue**
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	**N/A**	**Current Issue**
Backdoor-QV	**N/A**	**Current Issue**
Backdoor-QZ	**N/A**	**Current Issue**
BAT.Black	N/A	CyberNotes-2001-11
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
EIC.Trojan	**N/A**	**Current Issue**
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.StartPage	N/A	CyberNotes-2001-07
JS_ZOPA.A	**N/A**	**Current Issue**
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02

Trojan	Version	CyberNotes Issue #
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/PsychwardB	**N/A**	**Current Issue**
Troj/Slack	**N/A**	**Current Issue**
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAFEIN111.A	**N/A**	**Current Issue**
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_IRC_NETOL.A	**N/A**	**Current Issue**
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12

Trojan	Version	CyberNotes Issue #
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.Billrus.Texto	**N/A**	**Current Issue**
Trojan.Lornuke	**N/A**	**Current Issue**
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	**N/A**	**Current Issue**
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Blank.A	**N/A**	**Current Issue**
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	**N/A**	**Current Issue**
Y3K Rat	1.6	CyberNotes-2001-11

AOL.PWSteal.86016 (Alias: W95.SoFunny.Worm@m): This is a password-stealing Trojan horse that has worm capabilities. It is a Visual Basic program that replicates using America Online (AOL) software. It will not run under Windows NT/2000. When executed, the Trojan/worm performs the following actions:

- It copies itself as \Windows\Msdos423.exe.
- To enable itself to run at startup, it adds the value "msdos423 <Windows>\msdos423.exe" to the registry key:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- It drops the text file \Windows\Msdos423.ini to mark its presence. The Msdos423.ini file contains the following strings:
  [Setup]
  Copied=True
- The first time that the worm is executed, it may display the following string:
  /avcenter/graphics/w95.sofunny.worm@m.gif
- To remove itself from the Taskbar and run unnoticed, the worm registers itself as a Service process. This permits the worm to continue to run even after you log off.
- The worm retrieves the window handles of programs that are currently running. If it detects the AOL login window class names, it retrieves the handles of the child windows. This permits to the worm to steal the user's user name and password from the AOL login screen. Also, the W95.SoFunny.Worm@m is able to determine the currently logged-in user and the NetBIOS name of the compromised computer.
- Next, the worm sends the intercepted information to the virus author's anonymous e-mail address using one of the following Web-based mail servers:
  mail.yahoo.com
  mail.hotmail.com
  mail.angelfire.com
  That means that the worm may send out e-mail even if there is no e-mail software installed on the compromised computer.
- The worm uses AOL software to replicate, and it is distributed as one of the following:
  Sofunny.exe
  Love.exe

Artic (0.6 beta): This is a Trojan that is in early development; many of its features are not finished. It uses the GirlFriend Trojan Source code. The server features are:

- Chat with server
- Display bitmap
- Exit windows
- File manager
- Freeze windows
- Get info
- Get passwords
- Get screen shot
- Key logger on/off
- Monitor on/off
- Open browser
- Open/close CD-Rom
- PC speaker
- Play sound
- Send message
- Show/hide task bar
- Talk to server (using microphone)

Backdoor.Bionet.40a: This is a malicious backdoor Trojan. Its actions are similar to SubSeven, Netbus, and BackOrifice in that it allows unauthorized access to an infected computer and runs as a server application. When executed, it performs the following actions:

- To make itself unnoticeable even on slow computers, it assigns itself the lowest thread priority value.
- To remove itself from the Applications list in the Windows Task Manager, it registers itself as a Service process. This permits the Trojan to continue to run even after the user logs off.
- It copies itself as \Windows\System\Procmon.exe.
- To enable itself to run at startup, it adds the value " procmon \Windows\System\procmon.exe" to the registry key, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- Next, Backdoor.Bionet.40a sends the message "Victim is Online" to the ICQ pager of the virus author. This tells the remote computer that the infected computer is ready for remote administration.
- It then starts to accept and perform the remote commands from the client program through the configurable port. The remote administrator has full access to the file system of the infected computer. The Trojan permits the remote administrator to download or upload files from the remote computer, change the registry, and run commands and programs.

Backdoor-QT (Aliases: Backdoor-QT.cfg, Backdoor-QT.cli, Backdoor-QT.svr, BackDoor.Muska (AVP), MuSka52): This is a remote access Trojan written in Visual Basic 5. When run, it copies itself to the WINDOWS SYSTEM directory as UT3.EXE and creates a WIN.INI entry to load the program at startup:

run= C:\WINDOWS\system\UT3.EXE

A registry value is also created to load the Trojan at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Resolution=C:\WINDOWS\system\UT3.EXE

The Trojan opens TCP/IP ports 52, 53, and 54 on the victim's machine and sends the victim's IP address to a configured ICQ user. Once infected, the attacker can intercepts AOL Instant Messages, send messages, and upload files to the victim.

Backdoor-QV: This is a password stealing, remote-access Trojan. When run, it copies itself to the Windows System directory as RUNDLL32.EXE (note, there is a valid RUNDLL32.EXE file in the Windows directory). Three random registry keys are created in static locations with the same key value:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\%RandomName%=C:\WINDOWS\SYSTEM\RUNDLL32.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\%RandomName%=C:\WINDOWS\SYSTEM\RUNDLL32.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\%RandomName%=C:\WINDOWS\SYSTEM\RUNDLL32.EXE

Backdoor-QZ: This is an FTP server Trojan with IRC bot/flooder and remote mailing capabilities. When run, it copies itself to the Windows directory as an .EXE file using a random 4-character name. A registry run key is created to load the file at startup:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WinUpdate=%WinDir%\%trojan%.exe

Additionally the program masquerades as the Windows Update program. It uses the same icon as the valid application and firewall programs may alert that Windows Update is trying to access the Internet.

EIC.Trojan: This Trojan horse damages the hard drive boot sector. To attempt to avoid detection, the Trojan contains code that is very similar to the Standard Antivirus Test File (EICAR). Like one of the EICAR test files, it is 68 bytes in length. This appears to have been done to cause users to believe that it is the test file. This Trojan calls INT 13, and it uses the call to write junk data to the hard drive boot sector, preventing the computer from booting. It also writes junk data to other sectors of the hard drive, possibly damaging files and folders. *NOTE: This Trojan will not run under Windows NT or 2000.*

JS_ZOPA.A (Aliases: JS.ZOPA.A, ZOPA.A, ZOPA): This non-destructive JavaScript Trojan that uses an ActiveX component exploit to change the Internet Explorer start up page and search page to point to a specific URL. The Trojan also adds a shortcut file in the "Favorites" folder to point to the URL. It is exploited in Internet Explorer v5.5 and Microsoft Outlook where ActiveX objects and/or malicious scripts are automatically executed when certain Web sites are viewed or certain e-mails are opened.

Trojan.Billrus.Texto: This is a memory-resident Trojan horse written in Visual Basic. It has an icon that makes it look like an ordinary text file. Every 10 minutes, it checks for a disk in drive A. If it finds one, it deletes as many files as is necessary to ensure enough space on the disk to copy both itself and another necessary, larger file to the disk. The Trojan deletes the following files, and replaces them with copies of itself: Attrib.exe, Edit.com, Format.com, Deltree.exe, Ed.cab, Mscdex.exe, Appwiz.cpl, Attrib.com, and Deltree.com. The Trojan can also change its file name to one of 18 different names, such as Readme.exe, Texto.exe, and so on. The first time that it is run, it starts Notepad and displays the e-mail address of the Trojan author. The Trojan adds a value to the registry so that it is run when Windows starts. The 30th time that the Trojan is activated, it deletes all files on the drive C, and displays a message box titled "Uruguay" that contains the text "Billrus." .

TROJ_CAFEIN111.A (Alias: CAFEIN111, CAFEIN111.A): This server component of a backdoor Trojan installs itself in an infected system and thereafter, stays in memory. Once active in memory, it allows a remote hacker control over an infected computer.

TROJ_IRC_NETOL.A (Aliases: IRC-Worm.Netol, W32/Netol, Troj/Netol14, IRC_NETOL.A): This non-destructive Visual Basic Trojan appears as a screen saver program and propagates via the Internet Relay Chat client mIRC. It also acts as a backdoor Trojan that controls an infected user's mIRC session. Upon execution, it creates a copy of itself, NETOL.SCR in any of the following directories:

C:\
C:\Windows\
C:\Archivos de programa\

The worm component is copied to a file, mIRC.HST, in a target mIRC directory and then adds an entry in the <rfiles> section of mIRC.INI to define mIRC.HST as another remote initialization file. After this, the Trojan displays a fake error message in Spanish indicating that the screen saver program works only under DirectX version 8.5 Alpha:

Brain ProtecTor
Este protector de pantalla solo funciona con DirectX 8.5 Alpha

When the infected user starts a mIRC session, the Trojan loads mIRC.HST, which sends out copies of itself to other users who connect to the same channel. The Trojan also has a backdoor function that gives a remote hacker control to an infected user's mIRC session.

Trojan.Lornuke (Alias: Nuker.Lornuke): This Trojan can be used to perform malicious actions against other computers. It is a type of program that is usually referred to as a nuker program. It is used to send packets of data to a specific IP addresses of the attacker's choosing so as to greatly slow down a victim's system. The program "nukes" the victim's system by sending packets of data at a specified interval. The Trojan's programmer can control various options such as how often and to which port the data is sent. This program also contains a mass-IP nuker, which allows it to "nuke" any systems that share the same subnet.

Troj/PsychwardB (Alias: BackDoor-CA): This is a Backdoor Trojan horse. When the Trojan server is running on a computer, the computer is vulnerable to unauthorized access attacks from network locations. In order to gain access to the infected computer, an attacker has to run the Trojan client program. The Trojan server creates a copy of itself in the Windows directory and adds the registry value HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winvxd containing the name of the copy.

Troj/Slack (Aliases: Backdoor.Slackbot, DDOS/Slack): This is a backdoor Trojan horse which can be configured to connect to any IRC server. When the Trojan connects to an IRC server, it joins a pre-configured IRC channel and waits for further commands. The Trojan could be used to launch DDoS attacks by sending a large number of UDP packets to a target host. When the Trojan is run, it copies itself into the Windows directory with a random filename and changes the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Update so that this file runs on Windows startup. It also attempts to connect to a website to download an updated Trojan file.

Trojan.VBS.PWStroy (Alias: VBS/PWStroy): . This is a VBScript Trojan that can modify the Autoexec.bat file so that drive C is reformatted when the computer is restarted. It can also use Microsoft Outlook to send the logged in user's .pwl file (password file) to two e-mail addresses. This Trojan contains the comment line 'VBS.Dr.Trojan 2.1' at the top of the code. When the script is run, it does the following:

- It copies itself to the \Windows\System folder as Kernel32.vbs.
- Next, it adds the value 'System32' to the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run so that the Trojan runs when Windows is started.
- It then reads the registry to determine the name of the logged-on user. Using this information, the Trojan then attempts to locate a file in the \Windows folder that has the same file name as the user name and that has the .pwl extension.
- It starts Microsoft Outlook and sends the following message to two e-mail addresses:
  - Subject: PASSWORD
  - Message: PASSWORD FILE GOT>
  - Attachment: The .pwl file that contains the Windows logon password.
- Finally, with a 1-in-120 chance, this script modifies the Autoexec.bat file with instructions to format drive C. It the restarts the computer, which causes the Autoexec.bat file to run.

NOTE: If this payload is executed, it does not affect computers running Windows NT/2000 because they do not use the Autoexec.bat file when restarting.

VBS.Blank.A: This is a VBScript Trojan which can change the current Internet Explorer home page to the \Windows\AboutBlank.htm file. The script in the \Windows folder creates this file. AboutBlank.htm contains a link to the original Internet Explorer home page, so that it will appear that Internet Explorer has loaded the correct page when it starts. The file also automatically sends an ICQ message to a specific ICQ user whenever the home page is viewed.

W32.Leave.B.Worm: This Trojan/worm downloads components from Web sites and contains code to accept commands from IRC. The only differences between this threat and W32.Leave.Worm are the Web sites from which the components are downloaded, and that this threat is crafted to appear as a security bulletin from Microsoft. This threat arrives as an e-mail message written so that it appears to come from Microsoft as a security bulletin. The text of this message is as follows:

> Subject: Microsoft Security Bulletin MS01-037
> Message: The following is a Security Bulletin from the Microsoft Product Security Notification Service.
> Please do not reply to this message, as it was sent from an unattended mailbox.
>
> Title: Vulnerability in Windows systems allowing an upload of a serious virus.
> Date: 30 June 2001
> Software: Windows 2000
> Impact: Privilege Elevation
> Bulletin: MS01-037
> Microsoft encourages customers to review the Security Bulletin at:
> http://www.microsoft.com/technet/security/bulletin/MS01-037.asp
>
> Yesterday the Internet has seen one of the first of it's downfalls. A virus (no name assigned yet) has been released. One with the complexity to destroy data like none seen before.
>
> Systems affected:
>
> Microsoft Windows 95
> Microsoft Windows 95b
> Microsoft Windows 98
> Microsoft Windows 98/SE
> Microsoft Windows NT Enterprise
> Microsoft Windows NT Workstation
> Microsoft Windows Millennium Edition

Microsoft Windows 2000 Professional
Microsoft Windows 2000 Server
Microsoft Windows 2000 Advanced Server
Service packs up to Service Pack 6 for Windows NT 3/4 Systems.
Service pack 1 and 2 for windows 2000.

Issue:

Officials say this virus is unique in many ways. It spreads via new forms, such as using a new vulnerability in Windows 98 allowing already infected computers to upload (send files) to non-infected computers, this means that you do not have to download or visit a site to be infected with the virus. The infected computers are programmed to scan for computers running Windows 9x, and Windows 2000 and uploading the virus.